Blocking data for request from network involves requesting data via Clean Surf Server using predetermined filter criterion and acting as filter to distinguish unwanted data from tolerated data

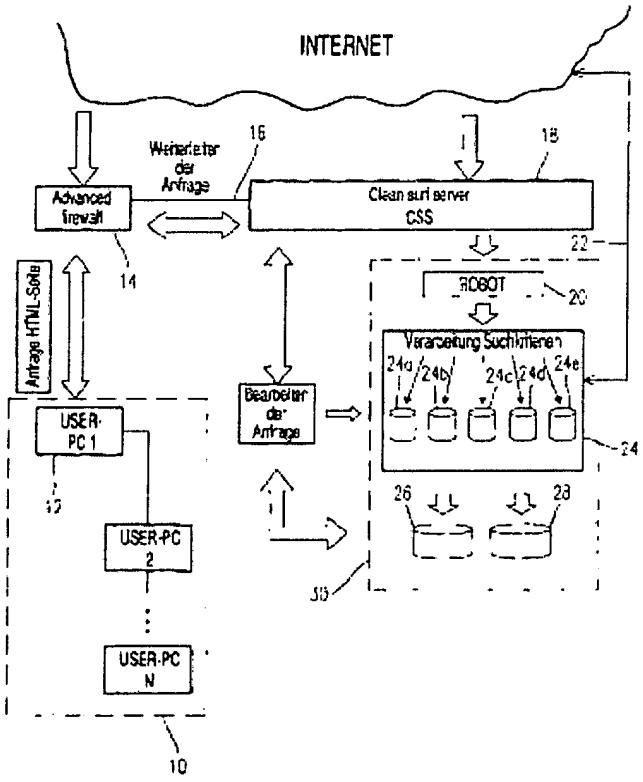
Patent number:	DE10024733
Publication date:	2001-11-22
Inventor:	SPEHR CLEMENTE (DE)
Applicant:	SPEHR CLEMENTE (DE)
Classification:	
- international:	H04L12/00; G06F12/14; G06F13/00; H04L12/22
- european:	G06F17/30W1F
Application number:	DE20001024733 20000519
Priority number(s):	DE20001024733 20000519

Also published as:

WO0190932 (A3)
WO0190932 (A2)

Abstract of **DE10024733**

The method involves requesting data from a network via a Clean Surf Server (18) using a predetermined filter criterion and acting as a filter server between an end user computer (12) and the network in order to distinguish unwanted data from data to be tolerated. The method is used in a firewall system (14) to prevent the reception of unwanted contents at several networked computers (10). Independent claims are also included for the following: a method of filtering data for request from a network, a use of the method to filter unwanted sequences from image or tone sequences or videos, a computer program, a computer program product and a computer system containing an arrangement for implementing the method.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 24 733 A 1**

(5) Int. Cl.[7]:
H 04 L 12/00
G 06 F 12/14
G 06 F 13/00
H 04 L 12/22

(21) Aktenzeichen: 100 24 733.4
(22) Anmeldetag: 19. 5. 2000
(43) Offenlegungstag: 22. 11. 2001

DE 100 24 733 A 1

(71) Anmelder:
Spehr, Clemente, 80469 München, DE

(74) Vertreter:
PAe Reinhard, Skuhra, Weise & Partner, 80801 München

(72) Erfinder:
gleich Anmelder

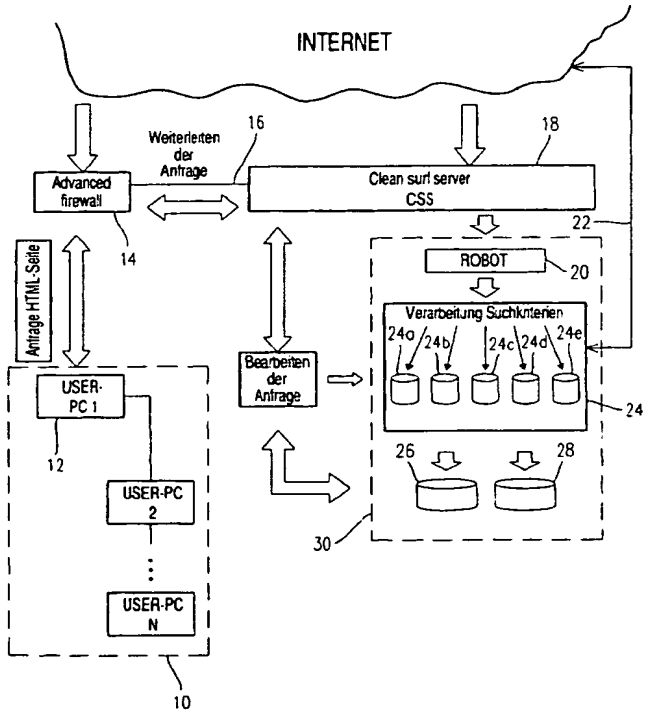
(56) Entgegenhaltungen:
DE 197 41 238 C2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Vorrichtung zum Abblocken von aus einem Netzwerk anforderbaren Daten

(57) Ein Verfahren und Vorrichtungen zum Abblocken von aus einem Netzwerk anforderbaren Resourcen mit unerwünschtem Inhalt, sowie ein Verfahren zum Ausfiltern solcher Daten aus einer beliebig großen Datenmenge wird vorgeschlagen. Angeforderte Webseiten werden beispielsweise vor dem Verbrauch beim Endbenutzer auf ihre Integrität hin kontrolliert. Die anforderbaren Informationsressourcen werden im wesentlichen vollautomatisch durch ein erfindungsgemäßes Filterprogramm beruhend auf Erkennung und gewichteter Bewertung einzelner "verdächtiger" Informationselemente untersucht und qualifiziert.



DE 100 24 733 A 1

Beschreibung

STAND DER TECHNIK

[0001] Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zum Abblocken von aus einem Netzwerk anforderbaren Daten mit unerwünschtem Inhalt sowie ein Verfahren zum Ausfiltern solcher Daten aus einer beliebig großen Datenmenge.

[0002] Obwohl auf beliebige Daten und Netzwerke anwendbar, werden die vorliegende Erfindung sowie die ihr zugrundeliegende Problematik in Bezug auf eine Situation erläutert, in der mehrere, miteinander vernetzte Endbenutzer-PCs einen Firewall Zugang zum Internet besitzen. Das Internet wird heutzutage von vielen Menschen genutzt. Es ist eine hervorragende, komplexe, unter Umständen einfach zu recherchierende Informationsressource für eine Vielfalt von Ressourcen, wie beispielsweise Texte, Bilder, Daten, Tonsequenzen oder Bildsequenzen beziehungsweise Kombinationen daraus, wie es beispielsweise in Videofilmen der Fall ist. Die Informationen werden dabei grundsätzlich auf Anforderung eines Endbenutzers von einer meist für die angeforderte Information spezifischen Datenquelle, einem Netzserver, zum Endbenutzer transportiert, wo sie entweder nur dargestellt oder auch gespeichert und weiterverarbeitet werden können.

[0003] Mit zunehmender Akzeptanz des Internets in weiten Kreisen von Wirtschaft und Bevölkerung haben sich die Inhalte der im Internet dargebotenen Webseiten stark diversifiziert: einerseits gibt es informative, sehr nützliche Informationen die für den Verbrauch beim Endbenutzer unproblematisch sind. Andererseits gibt es jedoch eine Vielzahl nicht gewünschter Informationen, beispielsweise Informationen, die thematisch im Bereich Sex, Hardcore, Kinderporno, Gewalt, oder auch reiner Werbung liegen.

[0004] Je nach Alter, Interessen und Hintergrund eines oder mehrerer Endbenutzer dieser Informationen ist es wünschenswert, bestimmte oder alle im Netz verfügbaren Informationen, die zu einem oder mehreren der vorgenannten Themen eindeutig zuzuordnen sind, auszufiltern, um den Endbenutzer nicht damit zu belasten.

[0005] Solche Informationen werden im folgenden als nicht gewünschte Informationen bezeichnet.

[0006] Es gibt freilich gewisse objektive Maßstäbe nach denen solche Informationen gefiltert werden könnten. Darunter fallen beispielsweise Informationen, in denen die Gewalt verherrlicht wird, die Kinderpornos zeigen, oder gewisse, moralisch stark bedenkliche Sex and Crime-Inhalte, um nur die wichtigsten zu nennen. Für solche Inhalte erscheint eine globale, klassische Indizierung angebracht. Das Problem dabei ist jedoch, wie solche Informationen, beispielsweise in Form von Webseiten wirksam vor dem Endbenutzer abgeblockt werden können. Ein weiterer Aspekt, der bei jenem Abblocken zu berücksichtigen ist, ist die Tatsache, daß ein und der selbe Inhalt nicht für alle Menschen gleich schädlich beziehungsweise unerwünscht ist. So gibt es beispielsweise Menschen, die sich durch Werbeblöcke oder Werbebanner kaum stören lassen oder aber Menschen, die auf die Einblendung solcher Werbemittel sehr sensibel reagieren. Auch kann ein erwachsener Mensch ein größeres Maß an den oben genannten Sex and Crime-Informationen verarbeiten, ohne daran Schaden zu nehmen, im Vergleich zu einem Kind. Da Kinder jedoch in zunehmendem Maße auch als Endbenutzer in Frage kommen, müssen Kinder beispielsweise selektiv vor unerwünschten oder verbotenen Inhalten geschützt werden.

[0007] Im Stand der Technik befindliche Möglichkeiten, selektiv bestimmte Inhalte dem Endbenutzer vorzuenthalten, sind nur über Texterkennung gegeben. Insbesondere kann dem Endbenutzer der Zugang nur zum PC als Maschine über ein Paßwort möglich sein, wobei das Paßwort auch beim Aufruf eines Browser-Programms verlangt werden kann.

[0008] Dies hat jedoch den Nachteil, daß der Endbenutzer auch keine für ihn nützlichen oder wertvollen Daten aus dem Netz ziehen kann.

VORTEILE DER ERFINDUNG

[0009] Das erfindungsgemäße Verfahren mit den Merkmalen des Anspruchs 1, das Verfahren mit den Merkmalen des Anspruchs 5 sowie die entsprechenden Vorrichtungen gemäß Ansprüchen 16 bis 19 weisen gegenüber den bekannten Lösungsansätzen den Vorteil auf, daß die Zugangskontrolle flexibler als bisher gestaltbar ist. Fordert der Endbenutzer beispielsweise aus dem Internet bestimmte Daten an, so werden diese Daten vor einer Darstellung beim Endbenutzer daraufhin untersucht, ob sie bestimmten, flexibel bestimmbaren Filterkriterien genügen oder nicht. Diese Filterkriterien werden dann als Basis dafür herangezogen, zu entscheiden, ob die Daten als "ungewünscht" vom Endbenutzer abzublokken sind, oder ob sie als tolerabel dem Endbenutzer zuführbar sind. Es wird also ein sogenannter Filterserver zwischen den Endbenutzer-PC und dem Informationsnetzwerk geschaltet, der vorzugsweise für eine Vielzahl von Endbenutzern gleichzeitig diese Filterfunktion realisiert. Das Ausfiltern besteht im wesentlichen aus einer Untersuchung der Daten hinsichtlich ihrer Integrität bezüglich der vorbestimmten, indizierten Themen, dem Qualifizieren der untersuchten Daten hinsichtlich dieser Integrität, dem Speichern dieser Daten und/oder deren Referenzen in einer Datenbank zusammen mit deren Beurteilungsergebnissen und der Entscheidung zwischen Abblocken oder Freigabe.

[0010] Wenn eine Firewall die Schnittstelle zu dem Informationsnetzwerk darstellt, kann diese in vorteilhafter Weise auch derart erweitert sein, daß die Entscheidung auf Abblocken oder Freigabe von ihr erstellt wird. Dies hat den Vorteil, daß Wartung und Pflege der Kriterien an einer einzigen Stelle einfach für eine Mehrzahl von Endbenutzern durchgeführt werden kann, wobei dies gleich in Kombination mit der im Stand der Technik vorhandenen Praxis der automatischen Virenkontrolle kombiniert werden kann. Im Falle der Nutzung des erfindungsgemäßen Verfahrens kann das erfindungsgemäße Filterverfahren auch entweder zwangsgesteuert oder vom Endbenutzer freiwillig steuerbar von seinem entfernt liegenden PC aus angestoßen werden. In vorteilhafter Weise kann die vorerwähnte Filterfunktion auch durch Computersysteme realisiert werden, die bei dem vom Endbenutzer gewählten Netzprovider eingesetzt werden.

[0011] Die der vorliegenden Erfindung zugrundeliegende Idee besteht darin, daß alle angeforderten Netzwerkinformationsressourcen, z. B. Webseiten aus dem worldwide web, vor dem Konsum beim Endbenutzer auf ihre Integrität hin kontrolliert werden. Dies kann zeitnah zur Anforderung geschehen, sollte aber zeitlich vorzugsweise von der Benutzeranforderung entkoppelt werden. Die anforderbaren Informationsressourcen werden im wesentlichen vollautomatisch durch ein erfindungsgemäßes Filterprogramm untersucht und qualifiziert. Diese Untersuchung läuft vorzugsweise steuerbar in verschiedenen Ebenen ab: Einerseits ist es sinnvoll, eine "schwarze Liste" mit Referenzen auf Adressen bestimmter Datenquellen zu führen, die bekanntermaßen ungewünschte Inhalte zur Verfügung stellen. Andererseits ist es sinnvoll, eine "grüne Liste" mit Referenzen auf Adressen bestimmter Datenquellen zu führen, die bekanntermaßen

gewünschte Inhalte zur Verfügung stellen.

[0012] Dies können beispielsweise die IP-Adressen der zugehörigen Webserver oder spezielle Webseiten-URLs sein, wenn als Informationsressource das Internet gilt. Diese einfache Form des Filterns benötigt dann lediglich einen Abgleich zwischen der vom Endbenutzer angeforderten Referenz mit den entsprechenden Listen.

[0013] Das erfindungsgemäß vorgeschlagene Verfahren ist jedoch wesentlich flexibler und wirksamer als ein solcher pauschaler Abgleich: denn bestimmte Elemente der aus dem Netzwerk stammenden Daten können einzeln identifiziert und mit einer Wichtung belegt abgespeichert werden. Dabei deckt die Wichtung die verschiedenen, oben genannten, indizierten Themenbereiche, wie zum Beispiel Gewalt, Porno, Sex and Crime, ab. Ziel ist es dabei, möglichst zuverlässig signifikante Informationen aus dem downgeloadeten Inhalt zu finden, die möglichst eindeutig den Schluß zulassen, daß der betreffende Inhalt als unerwünscht eingestuft werden kann. Ein nackter Hintern kann beispielsweise mit einem Wichtungsprozentsatz von 80% für den Themenbereich Sex, mit 30% für den Themenbereich Hardcore, mit 40% für den Themenbereich Kinderporno, mit 0% für Themenbereich Gewalt, ebenso 0% für Werbung belegt werden. Wird beispielsweise ein nacktes Knie als Bildelement identifiziert, so bekommt es nur einen Wichtungsprozentsatz von 20% für Sex und entsprechend reduzierte Prozentsätze für die anderen Themenbereiche.

[0014] Die von dem Filterprogramm benutzten Suchalgorithmen können dabei auf im Stand der Technik vorhandenen Scan-Funktionen für Bilder, Text und Sprache basieren. In vorteilhafter Weise können die entsprechenden Module direkt von dem erfindungsgemäßen Filterprogramm übernommen und aufgerufen werden. Es werden also für alle Informationskategorien wie beispielsweise Text, Bild, Audio und Video spezifische Elementelisten erzeugt, die jeweils eine möglichst vollständige Auflistung solcher Elemente beinhalten, die einen Beitrag dazu liefern könnten, eine Webseite, oder andere Informationen, die das zugehörige Element enthalten, als unerwünscht oder aber als tolerabel einzustufen. In der Textliste können beispielsweise vulgäre Ausdrücke in verschiedenen Sprachen stehen. In der Bildliste können beispielsweise eine Vielzahl von Ganzkörper-Nacktdarstellungen und die Darstellung einzelner, vorzugsweise nackter oder spärlich bekleideter Körperteile abgespeichert werden. In der Audio-Liste können verschiedene Geräusche gespeichert werden, die für einen oder mehrere der oben genannten Themenbereiche signifikant sind, beispielsweise Stöhnen. Einzelne (Stand-)Bilder bzw. Bildsequenzen von Videos können mit der o. g. Bildliste bearbeitet werden.

[0015] Die in dem Filterserver laufende Software sucht vorzugsweise automatisch in einem Grundmodus ständig das Internet ab, um möglichst aktuelle Informationen zu haben. Auch im Stand der Technik vorhandene Techniken der Erkennung von Werbung können hierbei sinnvoll zum Einsatz kommen. Bestimmte, häufig wiederkehrende Motive aller Kategorien können in vorteilhafter Weise als besonders typisch für die entsprechende Kategorie abgespeichert werden, um einerseits als Vergleichsmuster für ähnliche Muster zu dienen und andererseits, um sie bei einem wiederholten Auftreten schneller erkennen zu können, wodurch die Performance beim automatischen Absuchen der Webseiten gesteigert wird.

[0016] Je nach verfügbarem Speicherplatz und anderen Randbedingungen, beispielsweise den bevorzugten Ziel-Webseiten der angeschlossenen Endbenutzer werden entweder komplette Webseiten auf dem Filterserver selbst gespeichert oder nur Referenzen auf diese Daten, beispielsweise die URL oder andere, signifikante Adressangaben, je nach Netzwerktyp oder Informationsquelle.

[0017] In bevorzugter Weise werden die Qualifizierungsergebnisse für die einzelnen Web-Inhalte in einer oder mehreren Datenbanken systematisch abgelegt. Durch einen Auswertealgorithmus, der diese Informationen liest und noch weitere Informationen aus dem Umfeld der Webseite hinzunimmt, kann dann bezüglich einer vom Endbenutzer angeforderten Webseite programmgesteuert eine Entscheidung getroffen werden, ob die angeforderte Information als unerwünscht oder als tolerabel zu beurteilen ist. Ist sie unerwünscht, so wird die Anforderung nicht bedient und gegebenenfalls ein Hinweis an den Endbenutzer ausgegeben. Andernfalls wird die Information an den Benutzer ausgegeben.

[0018] In den Unteransprüchen finden sich vorteilhafte Weiterbildungen und Verbesserungen des jeweiligen Gegenstandes der Erfindung.

[0019] Gemäß einer bevorzugten Weiterbildung besteht das erfindungsgemäß vorgeschlagene System aus zwei Elementen, zum einen mit einer erweiterten Firewall als Front-End und einem sogenannten Clean Surf Server, im folgenden CSS abgekürzt, als Back-End. Dabei befindet sich das Front-End benutzerseitig auf dem Rechner, über den der Benutzer in das Internet kommt, sei es als Einzelplatz oder in einem lokalen Netzwerk. Der CSS ist in vorteilhafter Weise dem Netzprovider zugeordnet, wo er eine Vielzahl von Endbenutzern bedienen kann.

[0020] Gemäß einer bevorzugten Weiterbildung läuft das erfindungsgemäße Filterverfahren wenigstens zweistufig ab: In einer Vorstufe auf der Benutzerseite findet ein Abgleich zwischen benutzerangeforderten Inhalten mit als unerwünscht markierten und benutzerseitig gespeicherten Referenzen auf indizierte bzw. nicht-indizierte Inhalte statt. Bei einem Treffer in dieser "ersten schwarzen Liste" wird die Benutzeranforderung sofort abgelehnt, ohne den CCS zu kontaktieren. Wenn kein Treffer erfolgt und die URL noch nicht untersucht wurde, wird die Benutzeranforderung an den CCS zur Weiterbearbeitung weitergereicht. Ein flexibles, effizientes Verfahren folgt daraus, das vom Einzelplatz-PC bis hin zu großen Endbenutzer-Netzwerken skalierbar ist.

[0021] Gemäß einer bevorzugten Weiterbildung sind diese Referenzen Adressen bestimmter Datenquellen, die bekanntermaßen ungewünschte oder gewünschte Inhalte zur Verfügung stellen, also beispielsweise IP-Server-Adressen oder URL-Seiten-Adressierungen. Dies steigert die Performance, da die Antwortzeit auf die Benutzeranforderung hin sehr gering ist.

[0022] Gemäß einer bevorzugten Weiterbildung können die Daten Webseiten aus einem Netzwerk, insbesondere dem Internet und dem WorldWideWeb entsprechen. Diese Maßnahme trifft dann den derzeitigen Hauptanwendungsfall der vorliegenden Erfindung.

[0023] Gemäß einer bevorzugten Weiterbildung umfassen die Indexthemen wenigstens eines der folgenden Themen: Sex, Hardcore, Kinderporno, Gewalt, Werbung und Kreditkarten, und ebenso die Eingabemöglichkeit von Kreditkartennummern. Eine solche Ausgestaltung unerwünschter Themen bietet einen relativ objektiven moralischen Maßstab zum "Sauberhalten" der dem Benutzer dargebotenen Inhalte.

[0024] Gemäß einer bevorzugten Weiterbildung werden Kombinationen bestimmter Elemente mit für die Kombination typischen Wichtungswerten belegt und abgespeichert. Werden beispielsweise in einem heruntergeladenen Bild sowohl eine Peitsche als auch menschliche Nacktdarstellungen gefunden, so kann mit relativ großer Wahrscheinlichkeit darauf geschlossen werden, daß es sich um eine Webseite

mit Sado-/Maso-Inhalten handelt. Daher bekommt die Kombination Peitsche plus nackter Körperteil oder nackter Körper einen hohen Wichtungsfaktor im Themenbereich Sex and Crime beziehungsweise Hardcore. Eine Peitsche allein als erkanntes Bildelement würde noch nicht ausreichen, um die Webseite derart einzustufen, da Peitschen ja auch als Reitzubehör dienen. Auch nackte Körperteile beziehungsweise nackte oder spärlich bekleidete Ganzkörperdarstellungen rechtfertigen für sich gesehen noch nicht eine solche Klassifizierung, denn sie sind durchaus üblich bei der Präsentation von Bademode oder Damen- oder Herren-Unterbekleidung.

[0025] In vorteilhafter Weise können auch Kombinationen gebildet werden aus Elementen, die aus verschiedenen Kategorien stammen. Beispielsweise bekäme die Kombination "Stöhnen plus Nacktdarstellung" einen hohen Wichtungsfaktor für den Themenbereich Sex. Kämen dann noch Handschellen oder bestimmte andere, bekannte Sado-/Maso-Zubehörteile als weiteres Kombinationselement hinzu, so würde der Wichtungsfaktor für Sex wieder reduziert, der von Hardcore beziehungsweise Sex and Crime jedoch von 0% auf einen sehr hohen Wert erhöht werden.

[0026] In bevorzugter Weise können durch komplexe Abfragealgorithmen und umfassende Reservoirs an Elementen für jede einzelne Informationskategorie themenbereichsspezifisch verläßliche Filterungsergebnisse erzielt werden. Dabei versteht sich von selbst, daß in diese Abfragealgorithmen viel empirisches Wissen integriert werden sollte, damit diese eine optimale Wirksamkeit erzielen.

[0027] Gemäß einer bevorzugten Weiterbildung kann ein von einem Endbenutzer spezifiziertes Benutzerprofil hinsichtlich der Definition ungewünschter Daten zusätzlich bei der Auswertung berücksichtigt werden. Dieses Benutzerprofil kann dann in geeigneter Weise mit den vorgegebenen, "objektiven" Filterkriterien überlagert werden, um effektive, benutzerbezogene, subjektive Filterkriterien aufzustellen. Diese effektiven Kriterien ersetzen dann die oben beschriebenen, objektiven Kriterien. Diese Maßnahme eignet sich insbesondere, um das erfindungsgemäße Verfahren an verschiedene Altersgruppen der Endbenutzer anzupassen. So kann es für Erwachsene durchaus wünschenswert sein, Sexdarstellungen betrachten zu können. Andererseits sollte dieses Minderjährigen verwehrt sein, ebenso wie der Zugang zu Gewaltdarstellungen.

[0028] Gemäß einer bevorzugten Weiterbildung enthält das Benutzerprofil eine Wichtung der verschiedenen Indexthemen.

[0029] Dies ermöglicht eine einfach zu realisierende Überlagerung der subjektiven mit den objektiven Filterkriterien.

[0030] Gemäß einer bevorzugten Weiterbildung werden vom Benutzer abgehende Suchbegriffe oder Seitenanforderungen untersucht, ob sie den oben angegebenen objektiven Filterkriterien genügen. Insbesondere können solche Suchbegriffe auch gefiltert werden. In einem solchen Fall werden beispielsweise die URL-Angaben, die vom Endbenutzer eingegeben wurden, auf ihre Integrität hin untersucht, bevor das dahinterliegende Bild- oder Tonmaterial untersucht wird. Findet sich die angeforderte URL auf der schwarzen Liste, so wird der Zugriff verweigert und der Benutzer entsprechend informiert. Dies steigert die Performance.

[0031] Das erfindungsgemäße Verfahren kann in vorteilhafter Weise auch zum eigentlichen Ausfiltern unerwünschter Inhalte in Bildsequenzen oder Tonsequenzen oder in Videos für sich betrachtet herangezogen werden. Die Auswertemethode hängt dabei sowohl von der Darstellungsweise als auch von der Übertragungsart ab. Werden beispielsweise in einer Videoübertragung bei den Bildinformationen nur Änderungen gegenüber dem Bild davor übertragen, so muß das "Grundbild" auf seine Integrität hin untersucht werden. Wenn allerdings die Änderung ein Bildelement einführt, das auf der Indexliste steht, so kann die Wichtung nach dem oben angegebenen-Verfahren vollzogen werden.

[0032] Bei streaming-basierten Übertragungen ist es vorteilhaft, die Übertragung durch einen temporären Pufferspeicher laufen zu lassen, und unerwünschte Teilsequenzen entweder zu entfernen oder durch andere, unproblematische Teilsequenzen zu ersetzen. Dies hat den Vorteil, daß keine langweiligen Lücken bei der Wiedergabe der gestreamten Daten entstehen.

ZEICHNUNGEN

[0033] Ausführungsbeispiele der Erfindung sind in den Zeichnungen dargestellt und in der nachfolgenden Beschreibung näher erläutert.

[0034] Es zeigt

[0035] **Fig.** 1 eine schematische Blockdarstellung mit den wesentlichen technischen Funktionselementen und den wichtigsten Schritten während des Einsatzes des erfinderischen Verfahrens gemäß einem bevorzugten Ausführungsbeispiel.

BESCHREIBUNG DER AUSFÜHRUNGSBEISPIELE

[0036] **Fig.** 1 zeigt eine schematische Blockdarstellung mit den wesentlichen technischen Funktionselementen und den wichtigsten Schritten während des Einsatzes des erfinderischen Verfahrens gemäß einem bevorzugten Ausführungsbeispiel.

[0037] Ein unternehmensinternes Netzwerk **10** enthält eine Mehrzahl N von Endbenutzer-PCs, von denen zumindest einige zum Surfen im Internet eingerichtet sind. Für den vorliegenden Fall interessiert nur der oben eingezeichnete User-PC **1**. Er ist mit Bezugszeichen **12** versehen. Eine aus dem Stand der Technik bekannte Firewall-Netzwerkkomponente ist nun um einige erfindungsgemäße Funktionen erweitert. Diese Komponente ist mit Bezugszeichen **14** versehen. Die Primärfunktion der Firewall **14** bleibt die Ankopplung des Unternehmensnetzes an ein oder mehrere öffentliche Netze, wobei hier das Internet als Beispielsnetz dargestellt ist, siehe oberer Bereich der Figur.

[0038] Die Firewall-Komponente **14** ermöglicht eine Datenverbindung auf einer Datenleitung **16** zu einem sogenannten Clean Surf Server **18**, der als zwischengeschaltete Station dient, um einen direkten Kontakt zwischen Firewall **14** und Internet zu vermeiden. Dieser Server **18** wird im folgenden auch als CSS abgekürzt und arbeitet im wesentlichen als Filterserver.

[0039] Der Filterserver **18** ist mit einem Robot-Mechanismus **20** verbunden, der grundsätzlich unabhängig von einer Benutzeranfrage einen automatischen Zugang zum Internet besitzt und eine Vielzahl der dort angebotenen Inhalte auf Text, Ton, Dateninhalt, beispielsweise einem Vorhandensein von Viren, sowie Audio- oder Videosequenzen von Webseiten untersucht. Dies geschieht über eine separate Datenleitung **22**. Dieser Robot-Mechanismus enthält ein im Stand der Technik bekanntes Such-Programm, das nach einem vorgegebenen Netzwerksuchschema Webseiten einschließlich aller darauf befindlicher Links aufsuchen und deren Inhalte herunterladen kann. In vorteilhafter Weise arbeitet der Robot-Mechanismus in einem separat stehenden, leistungsfähigen Computer, der vorzugsweise von der Performance her frei skalierbar ist, um sich an den wachsenden Datenbestand im Internet gut anpassen zu können. Damit der Durchsatz gut ist, sollte die Datenleitung **22** vorzugsweise eine

sehr hohe Kapazität besitzen.

[0040] Der Robot-Computer **20** ist logisch und physikalisch mit einer Reihe von Datenbanken **24** verbunden, in denen für jede Informationskategorie eine große Anzahl von Suchkriterien gespeichert sind. Es gibt also für die Informationskategorie "Text" eine Datenbank **24a**, für die Kategorie "Bild" eine Datenbank **24b**, eine Audio-Datenbank **24c**, eine Video-Datenbank **24d** sowie optional eine Viren-Datenbank **24e**. In all diesen Datenbanken sind separat für jede Kategorie bestimmte Elemente gespeichert, die jeweils für ein oder mehrere, bestimmte, indizierte Themenbereiche relevant sind, wie es oben beschrieben wurde. Die Zusammenfassung mehrerer getrennter Datenbanken in eine einzige oder in eine niedrigere Anzahl von Datenbanken kann je nach Datenbanktyp und gewünschter Performance durchgeführt werden.

[0041] Der Robot-Mechanismus ist weiterhin logisch mit zwei Datenbanken **26** und **28** verbunden. Die Einheiten **20**, **24**, **26** und **28** bilden zusammen eine funktionsfähige Untereinheit **30**, die im Normalfall asynchron vom Filterserver **18** arbeitet und laufend das Internet nach neuen Inhalten hin untersucht, wobei in nicht separat dargestellten Suchverarbeitungs-Servern die gefundenen Webseiten mit den in den Datenbanken **24a**, . . ., **24e** gespeicherten Suchkriterien nach unerwünschten Inhalten durchsucht werden. Die Suchergebnisse werden dann in den beiden Datenbanken **26** und **28** abgelegt. Vorzugsweise werden gefundene Einzelelemente zusammen mit einer für sie typischen Wichtung in einer der beiden Datenbanken **26** oder **28** abgelegt.

[0042] Die Datenbank **26** enthält vorzugsweise die IP-Adressen bestimmter Webserver, die verbotene/unerwünschte Inhalte anbieten. Die Datenbank **28** enthält vorzugsweise verbotene/unerwünschte HTML-Seiten beziehungsweise solche HTML-Seiten, die wenigstens zum Teil unerwünschte Inhalte enthalten, sowie eine entsprechende Klassifizierung.

[0043] Wird beim automatischen Absuchen durch den Robot-Mechanismus beispielsweise eine HTML-Seite gefunden, die noch nicht in der Datenbank **28** abgespeichert ist, und die noch nicht auf ihre Integrität hin untersucht worden ist, so wird sie dem erfindungsgemäßen Untersuchungsverfahren unterworfen: Die gefundene HTML-Seite möge nun Textinformationen, Bild- und Audio-Informationen enthalten.

[0044] Vorzugsweise parallel zueinander werden nun verschiedene Prozesse gestartet: ein Text-Scan-Prozeß, ein Bildelemente-Scan-Prozeß und ein Audio-Elemente-Scan-Prozeß. Jeder der drei Prozesse isoliert nun, sofern möglich, einzelne Elemente in seiner jeweiligen Kategorie und vergleicht sie mit den in den Datenbanken **24** gespeicherten Suchkriterien. Als Textelement wird nun der Text-String "Ficken" gefunden. Gleichzeitig findet der Bild-Suchprozeß eine einzeln identifizierte Darstellung, die einer in der Bilddatenbank **24b** gespeicherten pornographischen Darstellung sehr ähnlich ist und eine pornographische Pose enthält. Des weiteren trifft der Audio-Suchprozeß auf ein Klangmuster, das sehr große Ähnlichkeit mit einem Klangmuster aufweist, der in der Audio-Datenbank **24c** als typisches "Stöhnen" abgespeichert ist. Jedes gefundene Element wird nun zusammen mit je einem Wichtungsfaktor für jeden der indizierten Themenbereiche in der entsprechenden Datenbank, hier der HTML-Datenbank **28** abgespeichert. Diese Verfahrensweise ermöglicht eine nachträgliche Änderung der Beurteilung durch Korrektur der Wichtungsfaktoren, wenn sich herausstellt, daß ein solcher Korrekturbedarf besteht. Eine solche nachträgliche Änderung kann dann erfolgen, ohne daß alle Seiten und Elemente neu untersucht werden müssen.

[0045] Auf der untersuchten Webseite werden als signifikante Elemente also der Text-String "Ficken", das Audio-Klangmuster eines Stöhnens sowie eine einzige pornographische Pose gefunden.

[0046] Der Text-String "Ficken" bekommt beispielsweise folgende Wichtungsfaktoren zugeteilt: Sex: 100%, Hardcore: 50%, Kinderporno: 40%, Gewalt: 10%, Werbung: 0%, Kreditkarte: 0%, da keine Eingabemöglichkeit für eine Kreditkartennummer gefunden wurde.

[0047] Das Audio-Muster "Stöhnen" bekommt in der Kategorie Sex 100%, bei Hardcore 60%, bei Kinderporno 30%, bei Gewalt 10%, bei Werbung 0% und bei Kreditkarte ebenfalls 0%.

[0048] Die pornographische Pose wird als Bildelement ebenfalls abgespeichert, wobei beispielsweise folgende Wichtungsfaktoren vergeben werden: Sex: 80%, Hardcore: 30%, Kinderporno: 40%, Gewalt: 0%, Werbung: 0% und Kreditkarte ebenfalls 0%.

[0049] Nach Bewertung der einzelnen Elemente liest ein komplexer Auswertealgorithmus die gespeicherten Wichtungsprofile und faßt sie zu einer Synthese zusammen, wobei vorzugsweise auch besondere Kombinationen einzelner Textelemente, wie es weiter oben erwähnt wurde, in besonderem Maße berücksichtigt werden.

[0050] Werden auf einer Webseite beispielsweise aber nur solche Elemente gefunden, die für sich gesehen und auch in Kombination miteinander keine eindeutigen Schlüsse zulassen, so kann auch die Umgebung der Webseite in die Wichtung eingehen: wenn in der hierarchischen Gliederung der Webseite weiter oben schon pornographische Inhalte gefunden wurden, oder wenn die URL der Webseite als pornographisch bekannt gilt, dann wird die Seite ebenfalls als unerwünscht abgeblockt, denn auf Pornoseiten finden sich mit einer hohen Wahrscheinlichkeit ausschließlich pornographische Abbildungen. Ein weiteres Indiz für eine Pornoseite sind Links auf bereits als Pornoseite erkannte Webseiten. Denn auch hier gibt es dann eine hohe Wahrscheinlichkeit, pornographisches Material zu finden.

[0051] Auch die IP-Adresse des Webservers könnte herangezogen werden, um von vornherein Webseiten auszuschließen oder um im Zweifelsfall Webseiten auszuschließen. Denn häufig liegen auf Webservern Webseiten, die jeweils einem einzigen Themenbereich aus den verbotenen Themen gewidmet sind. Dieser Fall tritt häufig bei illegalen Darstellungen, wie etwa Kinderporno oder rechtsradikalen, gewaltverherrlichenden Inhalten auf.

[0052] Darüber hinaus können im Zweifelsfall auch Menschen zur Beurteilung einer Webseite herangezogen werden.

[0053] Der Auswertealgorithmus kumuliert vorzugsweise die Wichtungsfaktoren aller auf einer Webseite gefundenen Elemente kategorieweise geordnet durch Multiplikation. Wenn beispielsweise fünf Elemente der Kategorie Gewalt gefunden werden, die die Wichtungsfaktoren 90%, 80%, 95%, 75% und 40% aufweisen, so werden die Prozentzahlen multipliziert, um ein Zwischenergebnis zu bilden. Dies wäre im vorliegenden Fall ein kumulativer Prozentsatz von 0,2052. Dieser wäre bereits als relativ hoch anzusehen, so daß die betroffene Seite als unerwünscht für das weitere Bearbeiten markiert wird.

[0054] Finden sich beispielsweise auf einer Webseite fünf Elemente mit den einzelnen Wichtungsfaktoren von 20%, 15%, 40%, 50% und 30%, also einer weit weniger verbotsträchtigen Elementesammlung, so ergibt sich ein kumulativer Prozentsatz von 0,0018. Der kumulative Prozentsatz liegt also bei der gleichen Anzahl von verwerteten Elementen um etwa zwei Zehnerpotenzen niedriger. Er würde daher nicht als unerwünscht markiert werden, sofern nicht andere Ausnahmetatbestände doch dafür sprechen. Es ist offen-

sichtlich, daß der Auswertealgorithmus die Anzahl der kumulierten Elemente bei seiner Beurteilung gebührend berücksichtigt, denn jeder Wichtungsfaktor, der kleiner als 1 ist, drückt den kumulativen Prozentsatz herunter. Daher kann beispielsweise durch Multiplizieren mit der Anzahl der kumulierten Elemente auf einfache Weise dafür eine Kompensation gefunden werden. Damit ergäbe sich beispielsweise für eine Webseite, die 5 Elemente mit einem jeweiligen Wichtungsfaktor von 90% aufweist, ein kumulativer Prozentsatz von 0,59, der dann mit 5 multipliziert einen Wert von etwa 3 ergäbe. Bei 10 gefundenen Elementen mit einem solchen Wichtungsfaktor ergäbe sich ein Wert von etwa 3,5, was die Ergebnisse gut vergleichbar macht.

[0055] Allgemein kann auch ein Bewertungsfaktor B durch die Formel

$$B = \text{Summe } (p_i E_i)/n$$

gewonnen werden, wobei pi die Wichtungsfaktoren darstellen, E_i die Elemente und n die Anzahl der Elemente.

[0056] Nach einer gewissen Vorlaufzeit, während der das Robot-System das Internet durchsucht hat bzw. auf bereits vorhandene Datenbanken zurückgreift und die Beurteilungsergebnisse in den beiden Datenbanken **26** und **28** abgespeichert hat, kann ein gewisser Teil der von dem User-PC **12** gemachten Anfragen an HTML-Seiten unter Berücksichtigung der Beurteilungsergebnisse bearbeitet werden. Dazu wird wie folgt vorgegangen: Die bereits untersuchten Webseiten werden als untersucht markiert. Der Endbenutzer am User-PC **12** definiert eine Anfrage nach einer bestimmten HTML-Seite auf seinem PC, indem er in einem Browser eine bestimmte Aktion durchführt, wie es durch Anklicken eines Links oder Eingabe einer URL der Fall sein kann.

[0057] Wenn die angeforderte Adresse noch nicht lokal als erwünscht oder unerwünscht klassifiziert wurde, wird die Anfrage wird nun in einem separaten Prozeß der erweiterten Firewall **14** bearbeitet und über die Leitung **16** zunächst an den Clean Surf Server CSS **18** weitergeleitet, der seinerseits die weitere Kontrolle bei der Bearbeitung übernimmt.

[0058] Zunächst wird festgestellt, ob die aktuell angeforderte Webseite bereits untersucht wurde oder nicht. Falls nicht, wird sie aus dem Internet downgeloadet und wie oben beschrieben beurteilt, wobei das Beurteilungsergebnis in der Datenbank **28** für HTML-Seiten abgespeichert wird.

[0059] Danach, ebenso wie in dem Fall, in dem die angeforderte Webseite bereits vor Absenden der Benutzeranforderung untersucht war, wird festgestellt, ob sie als unerwünscht gilt oder nicht. Dies kann durch Setzen eines Flags in dem entsprechenden HTML-Datensatz und Abfragen dieses Flags erfolgen. Je nach Untersuchungsergebnis kann dann der Zugang zur angeforderten Webseite ermöglicht oder abgeblockt werden.

[0060] Obwohl die vorliegende Erfindung anhand eines bevorzugten Ausführungsbeispiels vorstehend beschrieben wurde, ist sie darauf nicht beschränkt, sondern auf vielfältige Weise modifizierbar.

[0061] So kann beispielsweise der Clean Surf Server im Falle eines Abblockens an die Firewall zurückmelden, warum diese Seite nicht freigegeben worden ist, wobei die Firewall ab einer einstellbaren Häufigkeit von Anforderungen den Systemadministrator automatisch benachrichtigen kann, daß eine bestimmte Webseite in einem bestimmten Zeitintervall relativ häufig angefordert wurde. Weiterhin kann festgehalten werden, welche Webseiten angefordert wurde, welche Suchbegriffe verwendet werden, wieviele Verweigerungen es gab, etc.

[0062] Der Systemadministrator kann dann Maßnahmen ergreifen, um im Bedarfsfall die Webseite doch freizugeben oder, falls dies nicht beabsichtigt ist, andere Maßnahmen treffen, je nach Art der Webseite.

[0063] Das erfindungsgemäße Programm kann in vielerlei Ausgestaltungen installiert werden. Vorteilhaft ist eine spezielle Software oder Netzwerkkarte, auf die nur über ein geschütztes Paßwort zugegriffen werden kann, damit der Endbenutzer z. B. den Standard-Gateway oder Proxiserver von sich aus nicht umstellen kann. Dies kann auch als Kindersicherung dienen.

[0064] In vorteilhafter Weise können einzelne der vorhandenen Programmfunktionen des erfinderischen Verfahrens auch in einen herkömmlichen Web-Browser integriert sein.

[0065] Des weiteren kann in einer unter Umständen abgespeckten Version des erfinderischen Verfahrens die Funktion von Clean Surf Server **18** und Firewall **14** vollständig auf den End-User-PC gebracht werden, indem beispielsweise ein Verzeichnis aller nicht-erwünschten Inhalte, gekennzeichnet etwa durch die URLs oder die IP-Adresse von Webservern abgefragt wird, bevor eine Benutzeranforderung dem Endbenutzer zugänglich gemacht wird. Eine solche "schwarze Liste" kann beispielsweise auch in Form einer CD einzeln verkauft oder über das Internet oder sonstige mögliche Datenübertragungen downloadbar sein.

[0066] Des weiteren besteht die Möglichkeit, daß ein Endbenutzer, wenn er trotz Filterung eine unerwünschte Seite erhält, dies dem CSS rückmeldet, beispielsweise durch Betätigen eines eigenen Buttons in dem von ihm benutzten Browser.

[0067] Auch ein Bonussystem kann für verschiedene Zwecke in Kombination mit bestimmten der vorerwähnten Merkmale implementiert werden. Des weiteren können in einer speziellen Weiterbildung des erfinderischen Verfahrens solche Webseiten oder allgemeine Inhalte, die als hochgradig unerwünscht beurteilt wurden, automatisch einer separaten Behandlung unterzogen werden, die beispielsweise das Informieren einer zuständigen Behörde miteinschließt.

[0068] Mit der vorgeschlagenen Firewall-Erweiterung können ganze Netze ebenso wie Einzelrechner abgesichert werden. Das erfinderische Konzept ist nicht beschränkt auf das Absuchen verbotener Inhalte im Internet oder WorldWideWeb. Auch andere Netzwerke, wie beispielsweise Intranets können durchsucht werden.

[0069] Des weiteren können sogenannte Pushings und Pop-Ups, also ein automatisches Aufdrücken von Seiten beziehungsweise ein automatisches Aufmachen von Fenstern verhindert werden. Des weiteren können vorhandene Technologien wie Tunneling, also eine virtuelle Netzwerkprotokollverschachtelung mit implementiert werden. Auch kann die erweiterte Firewall und die CSS-Komponente auf einem Rechner oder System implementiert sein, der entfernt vom Endbenutzer-PC liegt und optional ebenfalls noch als Web-Server dient.

[0070] Des weiteren ist es möglich, durch Triggering-Mechanismen vom Stand der Technik zahlreiche andere Aktionen auszulösen, wenn eine Webseite als ungewünscht markiert wurde. So kann es beispielsweise sinnvoll sein, den Web-Master der zuständigen Seite zu informieren, beispielsweise durch automatisches Versenden einer eMail. Der Web-Master hat dann die Möglichkeit, Stellung zu nehmen oder die Seite möglicherweise zu verändern.

Bezugszeichenliste

10 Netzwerk(LAN)
12 Endbenutzer-PC
14 Firewall
16 Datenleitung

18 Clean Surf Server (CSS)
20 Robot-Mechanismus
22 separate Datenleitung
24–28 Datenbanken
30 Untereinheit

Patentansprüche

1. Verfahren zum Abblocken von aus einem Netzwerk anforderbaren Daten mit unerwünschtem Inhalt, enthaltend die Schritte,
Daten über einen vorbestimmte Filterkriterien verwendenden Clean Surf Server (CCS) (**18**) als Filterserver zwischen einem Endbenutzer-Computer (**12**) und dem Netzwerk aus diesem anzufordern,
um unerwünschte Daten von zu tolerierenden Daten zu unterscheiden.
2. Verfahren nach Anspruch 1, verwendet in einem Firewallsystem (**14**), um den Empfang unerwünschter Inhalte an mehreren, miteinander vernetzten Computern (**10**) zu verhindern.
3. Verfahren nach einem der vorstehenden Ansprüche, den weiteren Schritt enthaltend, in einer benutzerseitigen Vorstufe einen Abgleich zwischen benutzerangeforderten Inhalten mit als unerwünscht oder erwünscht markierten und benutzerseitig gespeicherten Referenzen durchzuführen,
bei einem Treffer die Benutzeranforderung abzulehnen, und
andernfalls die Anforderung an den CCS zur Weiterbearbeitung weiterzugeben.
4. Verfahren nach dem vorstehenden Anspruch, wobei die Referenzen Adressen bestimmter Datenquellen, die bekanntermaßen ungewünschte oder gewünschte überprüfbare Inhalte zur Verfügung stellen, als Serveradressen oder als Seitenadressen enthalten.
5. Verfahren zum Ausfiltern von aus einem Netzwerk anforderbaren Daten mit unerwünschtem Inhalt, enthaltend die Schritte,
Untersuchen der Daten hinsichtlich ihrer Erwünschtheit,
Qualifizieren der untersuchten Daten hinsichtlich ihrer Erwünschtheit,
Speichern von Netzwerkdaten und/oder deren Referenzen in einer Datenbank zusammen mit deren Beurteilungsergebnissen hinsichtlich unerwünschtem Inhalt,
Vorenthalter oder Freigeben von Benutzeranforderungen auf diese Daten je nach Maß ihrer Erwünschtheit.
6. Verfahren nach Anspruch 5, wobei die Daten Webseiten aus einem Netzwerk, insbesondere dem Internet entsprechen.
7. Verfahren nach Anspruch 5 oder 6, wobei die Daten wenigstens auf eines von Text, Bild, Ton, oder Virus-Befallenheit untersucht werden, und die Daten bezüglich ihrer Zugehörigkeit zu verschiedenen Indexthemen mit einer Wichtung beurteilt werden.
3. Verfahren nach einem der vorstehenden Ansprüche 5 bis 7, wobei die Indexthemen wenigstens eines von Sex, Hardcore, Kinderporno, Gewalt, Werbung, Eingabemöglichkeit von Kreditkartennummern umfassen.
9. Verfahren nach einem der Ansprüche 1 bis 8, wobei bestimmte Elemente der Daten einzeln identifiziert und mit einer Wichtung belegt abgespeichert werden.
10. Verfahren nach einem der Ansprüche 1 bis 9, wobei Kombinationen bestimmter Elemente mit für sie typischen Wichtungswerten belegt abgespeichert werden.
11. Verfahren nach einem der vorstehenden Ansprüche, weiter enthaltend den Schritt,
Auswerten eines Benutzerprofils hinsichtlich der Definition ungewünschter Daten,
Überlagern des Benutzerprofils mit dem Erwünschtheitsprofil zur Bestimmung eines subjektiven Erwünschtheitsprofils, um individuellen Filterkriterien zu genügen,
Vorenthalten oder Freigeben von Benutzeranforderungen auf diese Daten je nach Maß ihrer subjektiven Erwünschtheit,
Übermitteln einer Begründung im Falle des Vorenthaltens an den Benutzer.
12. Verfahren nach dem vorstehenden Anspruch, wobei das Benutzerprofil eine Wichtung verschiedener Indexthemen enthält.
13. Verfahren nach einem der vorstehenden Ansprüche, wobei vom Benutzer abgehende Suchbegriffe oder Seitenanforderungen hinsichtlich Anforderungen unerwünschten Inhalts untersucht werden und optionellerweise weitergemeldet werden.
14. Verwendung des Verfahrens nach einem der Ansprüche 5 bis 14 zum Ausfiltern unerwünschter Inhalte von Bildsequenzen oder Tonsequenzen oder Videos.
15. Verfahren nach dem vorstehenden Anspruch, wobei die Übertragung bei Streaming-basierten Übertragungen gepuffert verläuft und unerwünschte Teilsequenzen entfernt oder durch andere Teilsequenzen ersetzt werden.
16. Computerprogramm enthaltend Codeabschnitte zur Ausführung von Schritten des Verfahrens nach einem der Ansprüche 1 bis 4 oder 5 bis 15.
17. Computerprogrammerzeugnis, gespeichert auf einem computerlesbaren Datenträger, enthaltend computerlesbare Programmeinrichtungen, um einen Computer zur Ausführung von Schritten des Verfahrens nach einem der Ansprüche 1 bis 4 oder 5 bis 15 zu veranlassen, wenn es in eine Computer geladen wird.
18. Computersystem, enthaltend Mittel zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 4 oder 5 bis 15.
19. Computersystem, enthaltend Mittel zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 4 in Kombination mit dem Verfahren nach Ansprüchen 5 bis 15.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 100 24 733 A1
Int. Cl.⁷: H 04 L 12/00
Offenlegungstag: 22. November 2001

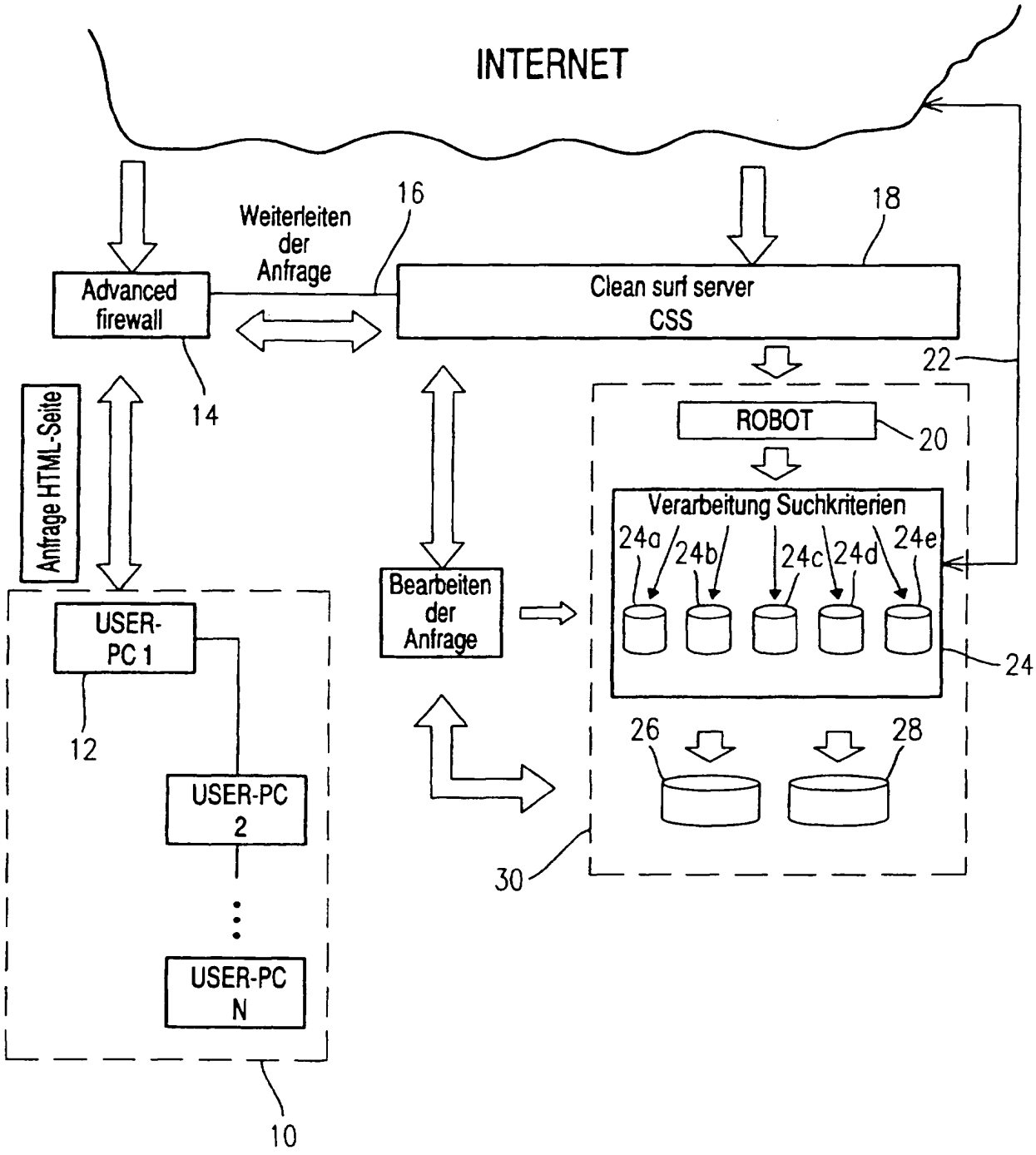


Fig. 1